

(E) A description of any incidents in which the Department of Justice assesses that United States courts and executive departments or agencies have relied on INTERPOL communications in contravention of existing law or policy to seek the detention of individuals or render judgments concerning their immigration status or requests for asylum, with holding of removal, or convention against torture claims and any measures the Department of Justice or other executive departments or agencies took in response to these incidents.

(F) A description of how the United States monitors and responds to likely instances of abuse of INTERPOL communications by member countries that could affect the interests of the United States, including citizens and nationals of the United States, employees of the United States Government, aliens lawfully admitted for permanent residence in the United States, aliens who are lawfully present in the United States, or aliens with pending asylum, withholding of removal, or convention against torture claims, though they may be unlawfully present in the United States.

(G) A description of what actions the United States takes in response to credible information it receives concerning likely abuse of INTERPOL communications targeting employees of the United States Government for activities they undertook in an official capacity.

(H) A description of United States advocacy for reform and good governance within INTERPOL.

(I) A strategy for improving interagency coordination to identify and address instances of INTERPOL abuse that affect the interests of the United States, including international respect for human rights and fundamental freedoms, citizens and nationals of the United States, employees of the United States Government, aliens lawfully admitted for permanent residence in the United States, aliens who are lawfully present in the United States, or aliens with pending asylum, withholding of removal, or convention against torture claims, though they may be unlawfully present in the United States.

(3) **FORM OF REPORT.**—Each report required under this subsection shall be submitted in unclassified form, but may include a classified annex, as appropriate. The unclassified portion of the report shall be posted on a publicly available website of the Department of State and of the Department of Justice.

(4) **BRIEFING.**—Not later than 30 days after the submission of each report under paragraph (1), the Department of Justice and the Department of State, in coordination with other relevant United States Government departments and agencies, shall brief the appropriate committees of Congress on the content of the reports and recent instances of INTERPOL abuse by member countries and United States efforts to identify and challenge such abuse, including efforts to promote reform and good governance within INTERPOL.

(f) **PROHIBITION REGARDING BASIS FOR EXTRADITION.**—No United States Government department or agency may extradite an individual based solely on an INTERPOL Red Notice or Diffusion issued by another INTERPOL member country for such individual.

(g) **DEFINITIONS.**—In this section:

(1) **APPROPRIATE COMMITTEES OF CONGRESS.**—The term “appropriate committees of Congress” means—

(A) the Committee on Foreign Relations and the Committee on the Judiciary of the Senate; and

(B) the Committee on Foreign Affairs and the Committee on the Judiciary of the House of Representatives.

(2) **INTERPOL COMMUNICATIONS.**—The term “INTERPOL communications” means any INTERPOL Notice or Diffusion or any entry into any INTERPOL database or other communications system maintained by INTERPOL.

**SA 1944.** Mr. RUBIO submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and Innovation in the National Science Foundation, to establish a regional technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place in subtitle A of title I of division F, insert the following:

**SEC. 61. PROHIBITED USE OF NIH FUNDING.**

Notwithstanding any other provision of law, no amounts made available to the National Institutes of Health may be used with respect to activities carried out by any company or its subcontractors or subsidiaries—

(1) over which control is exercised or exercisable by the Government of the People's Republic of China, a national of the People's Republic of China, or an entity organized under the laws of the People's Republic of China; or

(2) in which the Government of the People's Republic of China has a substantial interest.

**SA 1945.** Mr. LANKFORD (for himself, Mr. KING, and Ms. MURKOWSKI) submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and Innovation in the National Science Foundation, to establish a regional technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title III of division F, add the following:

**SEC. 63. LOAN GUARANTEES FOR PROJECTS THAT INCREASE THE DOMESTIC SUPPLY OF CRITICAL MINERALS.**

(a) **IN GENERAL.**—Section 1703(b) of the Energy Policy Act of 2005 (42 U.S.C. 16513(b)) is amended by adding at the end the following:

“(13) Projects that increase the domestic supply of critical minerals (as defined in section 7002(a) of the Energy Act of 2020 (30 U.S.C. 1606(a)), including through the production, processing, and recycling of critical minerals and the fabrication of mineral alternatives.”.

(b) **PROHIBITION ON USE OF PREVIOUSLY APPROPRIATED FUNDS.**—Amounts appropriated to the Department of Energy before the date of enactment of this Act shall not be made available for the cost of loan guarantees made under paragraph (13) of section 1703(b) of the Energy Policy Act of 2005 (42 U.S.C. 16513(b)).

(c) **PROHIBITION ON USE OF PREVIOUSLY AVAILABLE COMMITMENT AUTHORITY.**—

Amounts made available to the Department of Energy for commitments to guarantee loans under section 1703 of the Energy Policy Act of 2005 (42 U.S.C. 16513) before the date of enactment of this Act shall not be made available for commitments to guarantee loans for projects described in paragraph (13) of section 1703(b) of the Energy Policy Act of 2005 (42 U.S.C. 16513(b)).

**SA 1946.** Mr. GRAHAM submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and Innovation in the National Science Foundation, to establish a regional technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

**DIVISION G—COMBATING CHINESE THEFT OF TRADE SECRETS**

**SEC. 7001. SHORT TITLE.**

This division may be cited as the “Combating Chinese Purling of Trade Secrets Act” or the “CCP Trade Secrets Act”.

**TITLE I—INCREASED PENALTIES FOR VIOLATIONS OF SECTION 2512 OF TITLE 18, UNITED STATES CODE, INVOLVING A FOREIGN GOVERNMENT**

**SEC. 7101. MANUFACTURE, DISTRIBUTION, POSSESSION, AND ADVERTISING OF WIRE, ORAL, OR ELECTRONIC COMMUNICATION INTERCEPTING DEVICES PROHIBITED.**

(a) **IN GENERAL.**—Section 2512 of title 18, United States Code, is amended by adding at the end the following:

“(4) Any person who violates this section with the intent to benefit any government of a foreign country (as defined in section 1 of the Foreign Agents Registration Act of 1938, as amended (22 U.S.C. 611)), agency or instrumentality of a foreign state (as defined in section 1603(b) of title 28, United States Code), or agent of a foreign principal (as defined in section 1 of the Foreign Agents Registration Act of 1938, as amended (22 U.S.C. 611)) shall be fined under this title, imprisoned for not more than 20 years, or both.”.

(b) **SENTENCING ENHANCEMENT FOR FOREIGN INVOLVEMENT IN VIOLATIONS OF SECTION 2512 OF TITLE 18, UNITED STATES CODE.**—Pursuant to its authority under section 994 of title 28, United States Code, the United States Sentencing Commission shall review and amend the Federal sentencing guidelines to ensure that the guidelines provide an additional penalty increase of not fewer than 4 offense levels if the defendant violated section 2512 of title 18, United States Code, with the intent to benefit any government of a foreign country, agency or instrumentality of a foreign state, or agent of a foreign principal.

**TITLE II—PROTECTING U.S. BUSINESSES FROM FOREIGN TRADE SECRET THEFT**

**SEC. 7201. SHORT TITLE.**

This title may be cited as the “Protecting U.S. Businesses from Foreign Trade Secrets Theft Act of 2021”.

**SEC. 7202. PROHIBITION ON MISAPPROPRIATING U.S. TRADE SECRETS.**

(a) **IN GENERAL.**—Chapter 90 of title 18, United States Code, is amended by adding at the end the following:

**“§ 1840. Applicability to foreign persons**

“(a) **DEFINITIONS.**—In this section—

“(1) the term ‘critical technology’ has the meaning given the term ‘critical technologies’ in section 721 of the Defense Production Act of 1950 (50 U.S.C. 4565);

“(2) the term ‘designated Federal agency’ means—

“(A) the Department of Homeland Security;

“(B) U.S. Customs and Border Protection;

“(C) the Department of Commerce;

“(D) the Securities and Exchange Commission;

“(E) the Export-Import Bank of the United States;

“(F) the Department of State; and

“(G) the United States Patent and Trademark Office;

“(3) the term ‘foreign person’ means a person that is not a United States person;

“(4) the term ‘International Trade Commission’ means the United States International Trade Commission;

“(5) the term ‘offending foreign person’ means a foreign person—

“(A) who misappropriates a trade secret; and

“(B) with respect to whom a petition submitted under subsection (b)(1) satisfies the requirements under that subsection, as determined by the Attorney General;

“(6) the term ‘person’ means—

“(A) an individual; and

“(B) a corporation, business association, partnership, society, or trust, any other non-governmental entity, organization, or group, and any governmental entity operating as a business enterprise; and

“(7) the term ‘United States person’ means—

“(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States;

“(B) a corporation or other legal entity that is organized under the laws of the United States, any State or territory thereof, or the District of Columbia; and

“(C) a corporation or other legal entity—

“(i) organized under the laws of a jurisdiction outside of the United States; and

“(ii) with respect to which a United States person described in subparagraph (A) or (B)—

“(I) holds more than 50 percent of the equity interest by vote or value;

“(II) holds a majority of seats on the board of directors; or

“(III) otherwise controls the actions, policies, or personnel decisions.

“(b) PETITION FOR RELIEF.—

“(1) DEMONSTRATION OF MISAPPROPRIATION.—If an owner of a trade secret, who is a United States person, wishes to have the Attorney General or the head of the applicable designated Federal agency apply a penalty under subsection (c) to a foreign person who has misappropriated the trade secret, the owner shall submit to the Attorney General a petition demonstrating that—

“(A)(i) a court has entered a temporary restraining order, preliminary injunction, or final judgment under section 1836 of this title against the foreign person for misappropriating a trade secret of the owner;

“(ii) the International Trade Commission has issued a temporary exclusion order or final exclusion order under section 337 of the Tariff Act of 1930 (19 U.S.C. 1337) against the foreign person for misappropriating a trade secret of the owner; or

“(iii) an indictment has been issued under section 1831 or 1832 of this title against the foreign person for misappropriating a trade secret of the owner;

“(B) the trade secret described in the applicable clause of subparagraph (A) involves or is a component of critical technology; and

“(C) the remedies available to the owner under section 1836 of this title or section 337 of the Tariff Act of 1930 (19 U.S.C. 1337), as

applicable, are unlikely to provide complete relief to the owner because the foreign person has used or is reasonably likely to use the misappropriated trade secret in the home country of the foreign person or a third country, such that activities of the foreign person relevant to the determinations under subparagraph (A) take place outside the United States.

“(2) REVIEW.—Not later than 60 days after the date on which an owner who is a United States person submits a petition to the Attorney General under paragraph (1), the Attorney General shall determine whether the petition satisfies the requirements under that paragraph.

“(3) NOTIFICATION.—If the Attorney General determines under paragraph (2) that a petition satisfies the requirements under paragraph (1), the Attorney General shall so notify the head of each designated Federal agency not later than 30 days after the date of the determination.

“(4) SENSE OF CONGRESS.—It is the sense of Congress that if the Attorney General determines under paragraph (2) that a petition relating to a foreign person satisfies the requirements under paragraph (1), the Attorney General and the head of each designated Federal agency should impose 1 or more penalties on the foreign person under subsection (c), to the extent that the penalties are applicable.

“(c) PENALTIES.—

“(1) IN GENERAL.—Subject to paragraphs (2) and (3), not later than 90 days after the date on which the Attorney General provides notice to the head of each designated Federal agency under subsection (b)(3) with respect to an offending foreign person, the Attorney General or the head of a designated Federal agency, as applicable, may impose 1 or more of the following penalties on the offending foreign person:

“(A) IMPORT RESTRICTION.—The Commissioner of U.S. Customs and Border Protection may exclude from entry into the United States any articles produced by the offending foreign person.

“(B) EXPORT LICENSES.—

“(i) DUAL-USE EXPORTS.—The Secretary of Commerce may refuse to issue any specific license, or grant any other specific permission or authority, for the export, reexport, or in-country transfer of items to the offending foreign person under the Export Control Reform Act of 2018 (50 U.S.C. 4801 et seq.).

“(ii) DEFENSE ARTICLES AND DEFENSE SERVICES.—The Secretary of State may refuse to issue any license or other approval for the export of defense articles or defense services to the offending foreign person under the Arms Export Control Act (22 U.S.C. 2751 et seq.).

“(C) RESTRICTED PARTIES.—

“(i) COMMERCE LISTS.—The Secretary of Commerce may add the offending foreign person to one of the following lists maintained by the Bureau of Industry and Secretary of the Department of Commerce:

“(I) The Entity List set forth in Supplement No. 4 to part 744 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations.

“(II) The Denied Persons List maintained pursuant to section 764.3 of the Export Administration Regulations.

“(ii) TREASURY LIST.—The Secretary of the Treasury may add the offending foreign person to the list of specially designated nationals and blocked persons maintained by the Office of Foreign Assets Control of the Department of the Treasury.

“(D) SECURITIES REPORTING.—The Securities and Exchange Commission may determine whether the use by the offending foreign person of the misappropriated trade se-

cret is a reportable material condition in any filing by the offending foreign person required under applicable securities laws of the United States.

“(E) PATENT PROTECTION.—The Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office may prohibit the offending foreign person from applying for patent protection, being listed as an inventor on a patent application, or continuing a patent application under title 35, United States Code.

“(F) EXPORT-IMPORT BANK ASSISTANCE FOR EXPORTS TO FOREIGN PERSON.—The Export-Import Bank of the United States may refuse to approve the issuance of any guarantee, insurance, extension of credit, or participation in the extension of credit in connection with the export of any goods or services to the offending foreign person.

“(G) EXCLUSION OF CORPORATE OFFICERS.—The Secretary of State may deny a visa application, and the Secretary of Homeland Security may deny an application for admission to the United States, of any alien that the applicable Secretary determines is a corporate officer or principal of, or a shareholder with a controlling interest in, the offending foreign person.

“(H) OTHER PENALTIES.—The Attorney General or the head of a designated Federal agency—

“(i) may not procure, or enter into a contract for the procurement of, any goods or services from the offending foreign person;

“(ii) may prohibit, pursuant to notice issued by the Attorney General, a United States person from knowingly investing in or purchasing significant amounts of equity or debt instruments of the offending foreign person;

“(iii) may impose on a principal executive officer of the offending foreign person, or on an individual performing similar functions and with similar authorities as such an officer, any penalty under this subsection that could be imposed on the offending foreign person; and

“(iv) may impose on the offending foreign person any other penalty authorized under any provision of Federal law, as determined appropriate.

“(2) DURATION OF PENALTIES.—

“(A) TEMPORARY PENALTY.—If a court enters a temporary restraining order or preliminary injunction under section 1836 of this title against an offending foreign person for misappropriating a trade secret, the International Trade Commission issues a temporary exclusion order under section 337 of the Tariff Act of 1930 (19 U.S.C. 1337) against an offending foreign person for misappropriating a trade secret, or an indictment is issued under section 1831 or 1832 of this title against an offending foreign person for misappropriating a trade secret, the Attorney General or the head of a designated Federal agency may impose a penalty under paragraph (1) on the offending foreign person during the period during which the temporary restraining order, preliminary injunction, temporary exclusion order, or indictment remains in effect.

“(B) PERMANENT PENALTY.—If a court enters a final judgment under section 1836 of this title against an offending foreign person for misappropriating a trade secret, the International Trade Commission issues a final exclusion order under section 337 of the Tariff Act of 1930 (19 U.S.C. 1337) against an offending foreign person for misappropriating a trade secret, or an offending foreign person is convicted under section 1831 or 1832 of this title of misappropriating a trade secret, the Attorney General or the head of a designated Federal agency may permanently

impose a penalty under paragraph (1) on the foreign person.

“(3) PETITION FOR REVIEW.—

“(A) IN GENERAL.—If the Attorney General or the head of a designated Federal agency imposes a temporary penalty under paragraph (2)(A) or a permanent penalty under paragraph (2)(B) on an offending foreign person, the offending foreign person may submit to the Attorney General or the head of the designated Federal agency a petition for the revocation or modification of the penalty—

“(i) not later than 45 days after the date on which the penalty is imposed; or

“(ii) in the case of a permanent penalty, if the final judgment, final exclusion order, or conviction upon which the permanent penalty is based is reversed on appeal or otherwise vacated, not later than 45 days after the date of the reversal or vacatur.

“(B) CONTENTS OF PETITION.—

“(i) IN GENERAL.—An offending foreign person shall include in a petition submitted under subparagraph (A) a full written statement in support of the position of the offending foreign person, including a precise statement of why—

“(I) an insufficient basis exists for the penalty; or

“(II) the circumstances resulting in the penalty no longer apply.

“(ii) REMEDIAL STEPS.—An offending foreign person may, in a petition submitted under subparagraph (A), propose remedial steps that would negate the basis for the penalty.

“(C) DETERMINATION.—The Attorney General or the head of a designated Federal agency, as applicable, shall make a determination with respect to a petition submitted under subparagraph (A).

“(d) REPORT.—

“(1) IN GENERAL.—Not later than 1 year after the date of enactment of this section, and each year thereafter, the Attorney General, in coordination with the head of each designated Federal agency, shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report that—

“(A) with respect to the preceding year—

“(i) identifies foreign countries, state-owned and state-controlled entities, and other persons that engaged in the misappropriation of trade secrets owned by United States persons;

“(ii) describes any strategy used by a foreign country to undertake misappropriation of trade secrets owned by United States persons;

“(iii) identifies categories of technologies developed by, or trade secrets owned by, United States persons that were targeted for misappropriation;

“(iv) lists legal actions taken under section 1836 of this title, section 337 of the Tariff Act of 1930 (19 U.S.C. 1337), or section 1831 or 1832 of this title—

“(I) against an offending foreign person who misappropriated a trade secret owned by a United States person; and

“(II) as a result of which the products of the offending foreign person described in subclause (I) may never enter the United States; and

“(v) describes progress made in decreasing the prevalence of misappropriation of trade secrets owned by United States persons; and

“(B) recommends strategies to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives to decrease the misappropriation by foreign persons of trade secrets owned by United States persons.

“(2) FORM OF REPORT.—A report submitted under paragraph (1) shall be submitted in unclassified form but may contain a classified annex.”.

(b) TABLE OF SECTIONS.—The table of sections for chapter 90 of title 18, United States Code, is amended by adding at the end the following:

“1840. Applicability to foreign persons.”.

### TITLE III—COMBATING CYBERCRIME

#### SEC. 7301. SHORT TITLE.

This title may be cited as the “International Cybercrime Prevention Act”.

#### SEC. 7302. PREDICATE OFFENSES.

Part I of title 18, United States Code, is amended—

(1) in section 1956(c)(7)(D)—

(A) by striking “or section 2339D” and inserting “section 2339D”; and

(B) by striking “of this title, section 46502” and inserting “, or section 2512 (relating to the manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices) of this title, section 46502”; and

(2) in section 1961(l), by inserting “section 1030 (relating to fraud and related activity in connection with computers) if the act indictable under section 1030 is felonious,” before “section 1084”.

#### SEC. 7303. FORFEITURE.

(a) IN GENERAL.—Section 2513 of title 18, United States Code, is amended to read as follows:

“SEC. 2513. CONFISCATION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATION INTERCEPTING DEVICES AND OTHER PROPERTY.

“(a) CRIMINAL FORFEITURE.—

“(1) IN GENERAL.—The court, in imposing a sentence on any person convicted of a violation of section 2511 or 2512, or convicted of conspiracy to violate section 2511 or 2512, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

“(A) such person’s interest in any property, real or personal, that was used or intended to be used to commit or to facilitate the commission of such violation; and

“(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained or retained directly or indirectly as a result of such violation.

“(2) FORFEITURE PROCEDURES.—Pursuant to section 2461(c) of title 28, the provisions of section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) thereof, shall apply to criminal forfeitures under this subsection.

“(b) CIVIL FORFEITURE.—

“(1) IN GENERAL.—The following shall be subject to forfeiture to the United States in accordance with provisions of chapter 46 and no property right shall exist in them:

“(A) Any property, real or personal, used or intended to be used, in any manner, to commit, or facilitate the commission of a violation of section 2511 or 2512, or a conspiracy to violate section 2511 or 2512.

“(B) Any property, real or personal, constituting, or traceable to the gross proceeds taken, obtained, or retained in connection with or as a result of a violation of section 2511 or 2512, or a conspiracy to violate section 2511 or 2512.

“(2) FORFEITURE PROCEDURES.—Seizures and forfeitures under this subsection shall be governed by the provisions of chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 119 is amended by striking the item relating to section 2513 and inserting the following:

“2513. Confiscation of wire, oral, or electronic communication intercepting devices and other property.”.

#### SEC. 7304. SHUTTING DOWN BOTNETS.

(a) IN GENERAL.—Section 1345 of title 18, United States Code, is amended—

(1) in the heading, by inserting “AND ABUSE” after “FRAUD”;;

(2) in subsection (a)—

(A) in paragraph (1)—

(i) in subparagraph (B), by striking “or” at the end;

(ii) in subparagraph (C), by inserting “or” after the semicolon; and

(iii) by inserting after subparagraph (C) the following:

“(D) violating or about to violate section 1030(a)(5) of this title where such conduct has caused or would cause damage (as defined in section 1030) without authorization to 100 or more protected computers (as defined in section 1030) during any 1-year period, including by—

“(i) impairing the availability or integrity of the protected computers without authorization; or

“(ii) installing or maintaining control over malicious software on the protected computers that, without authorization, has caused or would cause damage to the protected computers;”; and

(B) in paragraph (2), in the matter preceding subparagraph (A), by inserting “, a violation described in subsection (a)(1)(D),” before “or a Federal”; and

(3) by adding at the end the following:

“(c) A restraining order, prohibition, or other action described in subsection (b), if issued in circumstances described in subsection (a)(1)(D), may, upon application of the Attorney General—

“(1) specify that no cause of action shall lie in any court against a person for complying with the restraining order, prohibition, or other action; and

“(2) provide that the United States shall pay to such person a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in complying with the restraining order, prohibition, or other action.”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 63 of title 18, United States Code, is amended by striking the item relating to section 1345 and inserting the following:

“1345. Injunctions against fraud and abuse.”.

#### SEC. 7305. AGGRAVATED DAMAGE TO A CRITICAL INFRASTRUCTURE COMPUTER.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

“§ 1030A. Aggravated damage to a critical infrastructure computer

“(a) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer, if such damage results in (or, in the case of an attempted offense, would, if completed, have resulted in) the substantial impairment—

“(1) of the operation of the critical infrastructure computer; or

“(2) of the critical infrastructure associated with such computer.

“(b) PENALTY.—Any person who violates subsection (a) shall, in addition to the term of punishment provided for the felony violation of section 1030, be fined under this title, imprisoned for not more than 20 years, or both.

“(c) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

“(1) a court shall not place any person convicted of a violation of this section on probation;

“(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation of section 1030;

“(3) in determining any term of imprisonment to be imposed for the felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such violation to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

“(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, if such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.

“(d) DEFINITIONS.—In this section—

“(1) the terms ‘computer’ and ‘damage’ have the meanings given the terms in section 1030; and

“(2) the term ‘critical infrastructure’ means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have catastrophic regional or national effects on public health or safety, economic security, or national security, including voter registration databases, voting machines, and other communications systems that manage the election process or report and display results on behalf of State and local governments.”.

(b) TABLE OF SECTIONS.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

“1030A. Aggravated damage to a critical infrastructure computer.”.

#### SEC. 7306. STOPPING TRAFFICKING IN BOTNETS; FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

(a) IN GENERAL.—Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) by striking paragraph (2) and inserting the following:

“(2)(A) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information, if—

“(i) the conduct was undertaken in furtherance of any felony violation of the laws of the United States or of any State, unless an element of such violation would require proof that the information was obtained without authorization or in excess of authorization; or

“(ii) the protected computer is owned or operated by or on behalf of a State or local governmental entity responsible for the administration of justice, public health, or safety, or owned or operated by or on behalf of the United States Government; or

“(B) intentionally accesses a computer without authorization, and thereby obtains information from any protected computer;”;

(B) by striking paragraph (6) and inserting the following:

“(6) knowing such conduct to be wrongful, intentionally traffics in any password or similar information, or any other means of access, further knowing or having reason to

know that a protected computer would be accessed or damaged without authorization in a manner prohibited by this section as the result of such trafficking;”;

(C) in paragraph (7), by adding “or” at the end; and

(D) by inserting after paragraph (7) the following:

“(8) intentionally traffics in the means of access to a protected computer, if—

“(A) the trafficker knows or has reason to know the protected computer has been damaged in a manner prohibited by this section; and

“(B) the promise or agreement to pay for the means of access is made by, or on behalf of, a person the trafficker knows or has reason to know intends to use the means of access to—

“(i) damage a protected computer without authorization; or

“(ii) violate section 1037 or 1343;”;

(2) in subsection (c)—

(A) in paragraph (2), by striking “, (a)(3), or (a)(6)” each place it appears and inserting “or (a)(3)”;

(B) in paragraph (3)—

(i) in subparagraph (A), by striking “(a)(4) or (a)(7)” and inserting “(a)(4), (a)(7), or (a)(8)”; and

(ii) in subparagraph (B), by striking “(a)(4), or (a)(7)” and inserting “(a)(4), (a)(7), or (a)(8)”; and

(C) in paragraph (4)—

(i) in subparagraph (C)(i), by striking “or an attempt to commit an offense”; and

(ii) in subparagraph (D), by striking clause (ii) and inserting the following:

“(ii) an offense, or an attempt to commit an offense, under subsection (a)(6);”;

(3) in subsection (e)—

(A) by striking paragraph (6) and inserting the following:

“(6) the term ‘exceeds authorized access’ means—

“(A)(i) to access a computer with authorization and thereby to knowingly obtain information from such computer that the accessor is not entitled to obtain; or

“(ii) to knowingly obtain any information from such computer for a purpose that is prohibited by the computer owner; and

“(B) provided that the limitation on access to or use of the information is not based solely on the terms governing use of an on-line service by customers or subscribers thereof, including terms set forth in an acceptable use policy or terms of service;”;

(B) by striking paragraph (10);

(C) by redesignating paragraphs (11) and (12) as paragraphs (10) and (11), respectively;

(D) in paragraph (10), as so redesignated, by striking “and”;

(E) in paragraph (11), as so redesignated, by striking the period at the end and inserting a semicolon; and

(F) by adding at the end the following:

“(12) the term ‘online service’—

“(A) means an electronic communication service (as defined in section 2510) to the public, a remote computing service (as defined in section 2711), or other service that provides content or computing services to the public over the Internet; and

“(B) does not include an enterprise service;”

“(13) the term ‘enterprise service’ means any electronic communication service (as defined in section 2510) to the public, remote computing service (as defined in section 2711), or other service that provides content or computing services to the public for which the user, customer, or subscriber has paid, or on whose behalf has been paid, more than \$10,000 in a calendar year in exchange for the right to access or use the service; and

“(14) the term ‘traffic’, except as provided in subsection (a)(6), means transfer, or otherwise dispose of, to another as consideration

for the receipt of, or as consideration for a promise or agreement to pay, anything of pecuniary value.”;

(4) in subsection (g), in the first sentence, by inserting “, except for a violation of subsection (a)(6),” after “of this section”; and

(5) by striking subsections (i) and (j) and inserting the following:

“(i) CRIMINAL FORFEITURE.—

“(1) IN GENERAL.—The court, in imposing a sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

“(A) such person’s interest in any property, real or personal, that was used or intended to be used to commit or to facilitate the commission of such violation; and

“(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained or retained, directly or indirectly, as a result of such violation.

“(2) FORFEITURE PROCEDURES.—Pursuant to section 2461(c) of title 28, the provisions of section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) thereof, shall apply to criminal forfeitures under this subsection.

“(j) CIVIL FORFEITURE.—

“(1) IN GENERAL.—The following shall be subject to forfeiture to the United States in accordance with chapter 46, and no property right shall exist in them:

“(A) Any property, real or personal, used or intended to be used, in any manner—

“(i) to commit, or facilitate the commission of, a violation of this section; or

“(ii) in a conspiracy to violate this section.

“(B) Any property, real or personal, constituting or traceable to the gross proceeds taken, obtained, or retained in connection with or as a result of—

“(i) a violation of this section; or

“(ii) a conspiracy to violate this section.

“(2) FORFEITURE PROCEDURES.—Seizures and forfeitures under this subsection shall be governed by the provisions of chapter 46 that apply to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—Section 7431(e)(3) of the Internal Revenue Code of 1986 is amended by striking “subparagraph (B)” and inserting “subparagraph (B)(iii)”.

#### TITLE IV—ESPIONAGE, THEFT OF TRADE SECRETS, AND IMPROPER INTERFERENCE IN UNITED STATES ELECTIONS

##### SEC. 7401. ESPIONAGE, THEFT OF TRADE SECRETS, THEFT OF INTELLECTUAL PROPERTY, INVOLVEMENT IN COMMERCIAL FRAUD SCHEMES, AND IMPROPER INTERFERENCE IN UNITED STATES ELECTIONS.

(a) DEFINITIONS.—Section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)) is amended by adding at the end the following:

“(53)(A) The term ‘espionage’ means conduct—

“(i) in violation of—

“(I) the Act of June 15, 1917 (40 Stat. 217, chapter 30) (commonly known as the ‘Espionage Act of 1917’);

“(II) chapter 90 of title 18, United States Code (commonly known as the ‘Economic Espionage Act of 1996’); or

“(III) any other Federal criminal law relating to an activity described in clause (ii); or

“(ii)(I) by an alien who is under the direction of—

“(aa) a foreign government; or

“(bb) an intermediary individual or entity that seeks to serve, support, or benefit a foreign government; and

“(II) with respect to confidential information, that constitutes—

“(aa) stealing or, without authorization, appropriating, taking, carrying away, concealing, or, by fraud, artifice, or deception, obtaining such information;

“(bb) without authorization, copying, duplicating, sketching, drawing, photographing, downloading, uploading, altering, destroying, photocopying, replicating, transmitting, delivering, sending, mailing, communicating, or conveying such information; or

“(cc) receiving, buying, or possessing such information, knowing that the information has been stolen or appropriated, obtained, or converted without authorization.

“(B) The term ‘espionage’ includes economic espionage.

“(54) The term ‘improper interference in a United States election’ means conduct by an alien that—

“(A)(i) violates Federal criminal, voting rights, or campaign finance law; or

“(ii) is under the direction of—

“(I) a foreign government; or

“(II) an intermediary individual or entity that seeks to serve, support, or benefit a foreign government; and

“(B) interferes with a general or primary Federal, State, or local election or caucus, including—

“(i) the campaign of a candidate; and

“(ii) a ballot measure, including—

“(I) an amendment;

“(II) a bond issue;

“(III) an initiative;

“(IV) a recall;

“(V) a referral; and

“(VI) a referendum.

“(55) The term ‘theft of a trade secret’ means conduct—

“(A) in violation of—

“(i) chapter 90 of title 18, United States Code (commonly known as the ‘Economic Espionage Act of 1996’); or

“(ii) any other Federal criminal law relating to an activity described in subparagraph (B); or

“(B)(i) by an alien who is under the direction of—

“(I) a foreign government; or

“(II) an intermediary individual or entity that seeks to serve, support, or benefit a foreign government; and

“(ii) with respect to a trade secret relating to a product or service used or intended for use in interstate or foreign commerce, that constitutes—

“(I) stealing or, without authorization, appropriating, taking, carrying away, concealing, or, by fraud, artifice, or deception, obtaining such trade secret for the economic benefit of any person other than the owner of the trade secret;

“(II) without authorization, copying, duplicating, sketching, drawing, photographing, downloading, uploading, altering, destroying, photocopying, replicating, transmitting, delivering, sending, mailing, communicating, or conveying such trade secret; or

“(III) receiving, buying, or possessing such trade secret, knowing that the trade secret has been stolen or appropriated, obtained, or converted without authorization.”.

(b) INADMISSIBILITY.—Section 212(a)(3) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)) is amended by adding at the end the following:

“(H) ESPIONAGE AND THEFT OF TRADE SECRETS.—An alien is inadmissible if a consular officer, the Secretary of Homeland Security, the Secretary of State, or the Attorney General knows, or has reasonable grounds to believe—

“(i) the alien is seeking admission or sought admission to the United States to engage in espionage or theft of a trade secret;

“(ii) the alien has engaged or intends to engage in espionage or theft of a trade secret; or

“(iii) the affiliation or activities of the alien with, or the control of the alien by, an individual, an entity, or a funding mechanism known or reasonably believed to be engaged in, or to have the intention of engaging in, espionage or theft of a trade secret.

(I) IMPROPER INTERFERENCE IN A UNITED STATES ELECTION.—Any alien who a consular officer, the Secretary of Homeland Security, the Secretary of State, or the Attorney General knows, or has reasonable grounds to believe, is seeking admission to the United States to engage in improper interference in a United States election, or who has engaged in improper interference in a United States election, is inadmissible.”.

(c) DEPORTABILITY.—Section 237(a) of the Immigration and Nationality Act (8 U.S.C. 1227(a)) is amended by adding at the end the following:

“(8) ESPIONAGE AND THEFT OF TRADE SECRETS.—Any alien who has engaged, is engaged, or at any time after admission engages in espionage or theft of a trade secret is deportable.

“(9) IMPROPER INTERFERENCE IN A UNITED STATES ELECTION.—Any alien who has engaged, is engaged, or at any time after admission engages in improper interference in a United States election is deportable.”.

#### SEC. 7402. VISA AND NONIMMIGRANT STATUS RESTRICTIONS.

(a) PERIOD OF AUTHORIZED STAY FOR CERTAIN CITIZENS AND NATIONALS OF THE PEOPLE'S REPUBLIC OF CHINA.—Section 214(a)(2) of the Immigration and Nationality Act (8 U.S.C. 1184(a)(2)) is amended by adding at the end the following:

“(C)(i) The period of authorized stay for a citizen or national of the People's Republic of China who seeks admission to the United States as a nonimmigrant described in subparagraph (F), (J), or (M) of section 101(a)(15) to study, research, teach, or work in any field described in the most recent technology alert list of the Department of State or in section 221(j)(1)—

“(I) shall be—

“(aa) a fixed period of not more than 4 years; or

“(bb) the length of the program identified on the Form I-20, Certificate of Eligibility for Nonimmigrant Student Status, or the Form DS-2019, Certificate of Eligibility for Exchange Visitor Status, as applicable, of such citizen or national of the People's Republic of China; and

“(II) may be extended by the Secretary of Homeland Security for 1 or more additional periods of not more than 2 years.

“(ii) This subparagraph shall not apply to any national of Hong Kong or Macau.”.

(b) PROHIBITION ON ISSUANCE OF VISAS TO CERTAIN CITIZENS AND NATIONALS OF THE PEOPLE'S REPUBLIC OF CHINA.—Section 221 of the Immigration and Nationality Act (8 U.S.C. 1201) is amended by adding at the end the following:

“(j) PROHIBITION ON ISSUANCE OF VISAS TO CERTAIN CITIZENS AND NATIONALS OF THE PEOPLE'S REPUBLIC OF CHINA.—

“(1) IN GENERAL.—The Secretary of State shall deny a visa to, and the Secretary of Homeland Security shall not admit into the United States, or grant a change of nonimmigrant status to, an alien who is a cit-

izen or national of the People's Republic of China if the Secretary of State or the Secretary of Homeland Security determines that the alien—

“(A) presents a risk to national security; or

“(B) otherwise seeks to enter the United States to participate in graduate-level coursework or research at an institution of higher education (as defined in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a))) in a field described in paragraph (2).

“(2) FIELDS DESCRIBED.—The fields described in this paragraph are—

“(A) the military or intelligence sector;

“(B) the energy sector;

“(C) nuclear science or nuclear engineering;

“(D) high-end numerical control machinery and robotics;

“(E) autonomous systems or machine learning;

“(F) artificial intelligence;

“(G) production and application of high-performance medical devices;

“(H) semiconductors;

“(I) new energy vehicles;

“(J) mobile phone technology;

“(K) next-generation information technology;

“(L) aviation, aeronautics, or space;

“(M) biomedicine; and

“(N) any related field, as determined by the Secretary of State or the Secretary of Homeland Security.

“(3) TERMINATION OF STATUS.—

“(A) IN GENERAL.—With respect to an alien who is a citizen or national of the People's Republic of China who has been admitted to the United States as a nonimmigrant described in subparagraph (F), (J), or (M) of section 101(a)(15), the Secretary of Homeland Security shall terminate the status and employment authorization of, and revoke any petition approval of or on behalf of, the alien if the Secretary determines that after such admission the alien—

“(i) has engaged in an activity or affiliation that presents a risk to national security; or

“(ii) has changed his or her program, course of study, research, or employment to graduate-level coursework or research at an institution of higher education in a field described in paragraph (2).

“(B) FAILURE TO MAINTAIN NONIMMIGRANT STATUS.—Any change or attempted change described in subparagraph (A) shall be considered to be a failure to maintain nonimmigrant status under this Act.

“(4) INAPPLICABILITY TO NATIONALS OF HONG KONG AND MACAU.—This subsection shall not apply to any national of Hong Kong or Macau.”.

(c) APPLICABILITY.—The amendments made by this section shall apply with respect to—

(1) any visa application filed on or after the date of the enactment of this Act; and

(2) the status of any alien, except for a national of Hong Kong or Macau, who—

(A) is a citizen or national of the People's Republic of China, regardless of the country of the passport presented by, or the country of residence of, the alien;

(B) before, on, or after the date of the enactment of this Act, has been or is admitted to the United States as a nonimmigrant described in subparagraph (F), (J), or (M) of section 101(a)(15) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)); and

(C) has changed or changes his or her program, course of study, research, or employment to graduate-level coursework or research at an institution of higher education (as defined in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a))) in a

field described in section 221(j)(1) of the Immigration and Nationality Act (as added by subsection (b)).

# **TITLE V—GOVERNMENT-FUNDED RESEARCH PROJECTS**

## **SEC. 7501. FINDINGS.**

Congress find the following:

(1) The People's Republic of China (referred to in this subsection as "the PRC" or "China") poses an existential threat to the economic interests and national security of the United States, in part due to the continued efforts of the PRC to steal sensitive technology and proprietary information from companies, academic institutions, and other organizations of the United States through economic espionage and other forms of nontraditional espionage.

(2) The PRC, through the Chinese Communist Party (referred to in this subsection as the "CCP"), has long had an interest in replacing the United States as the world's foremost superpower. China takes a holistic approach towards achieving its long-term goals, which are rooted in the concept of a comprehensive national power, including achieving dominance in economics, military affairs, science and technology, education, and global influence.

(3) Nontraditional forms of espionage serve as primary tools to further the goals of the CCP. Those tools include talent recruitment programs designed to recruit Chinese nationals to acquire knowledge about—and, often, steal—valuable and sensitive research at universities and research institutions abroad, and to lure foreign experts to China to work on key strategic programs. More broadly, the PRC uses mergers and acquisitions or joint ventures as a means to gain access to high-level technology, uses cyber intrusions to steal information, and uses front companies for PRC-related entities to acquire export-controlled technology.

(4) In 2015, President Xi Jinping of the PRC released the "Made in China 2025" initiative, a 10-year plan to update the manufacturing base of China by developing the following 10 high-tech industries:

(A) Electric cars and other new energy vehicles.

(B) Next-generation information technology and telecommunications.

(C) Advanced robotics and artificial intelligence.

(D) Aerospace equipment.

(E) Bio-medicine and high-end medical equipment.

(F) Ocean engineering equipment and high-end vessels.

(G) High-end rail transportation equipment.

(H) Electrical equipment.

(I) Farming machines.

(J) New materials, such as polymers.

(5) In attempting to overtake the United States and achieve its Made in China 2025 goals, China has systematically sought to identify areas of American innovation, education, and technology that could be replicated, stolen, or appropriated.

(6) The very nature of the open society of the United States—a free market economy that incentivizes creativity and ingenuity and promotes the free flow of capital and ideas, a higher education system and scientific research community that encourages collaboration domestically and internationally, and a liberal democratic government that lacks a top-down, authoritarian structure—creates opportunities for the PRC to target the United States in ways that are either not adequately protected or not even anticipated as possible threats.

(7) The Director of the Federal Bureau of Investigation has assessed that "there's no country that's even close" to the PRC when

it comes to foreign espionage, in traditional or nontraditional forms.

(8) As the 2018 Foreign Economic Espionage in Cyberspace report of the National Counterintelligence and Security Center (commonly known as the "NCSC") stated, China has expansive efforts in place to acquire United States technology, including sensitive trade secrets and proprietary information. China continues to use cyber espionage to support its strategic development goals—science and technology advancement, military modernization, and economic policy objectives. Chinese companies and individuals often acquire United States technology for commercial and scientific purposes.

(9) In April 2020, the Office of the United States Trade Representative (referred to in this subsection as the "USTR") issued its annual Special 301 Report, in which the USTR reviews the state of intellectual property protection and enforcement in trading partners of the United States around the world. The USTR continues to place China on the Priority Watch List, which reflects "United States concerns with China's system of pressuring and coercing technology transfer, and the continued need for fundamental structural changes to strengthen IP protection and enforcement, including as to trade secret theft, obstacles to protecting trademarks, online piracy and counterfeiting, the high-volume manufacturing and export of counterfeit goods, and impediments to pharmaceutical innovation."

(10) The theft of intellectual property, trade secrets, sensitive technology, and scientific and other academic research all contribute to China's goal of achieving preeminent superpower status. China's failure to respect intellectual property rights, failure to adhere to the rule of law, and efforts to obtain intellectual property, trade secrets, technology, and research through improper or illicit means all pose a significant economic and national security threat to the United States.

(11) In recent years, China has increased its use of nontraditional espionage to target colleges and universities in the United States, particularly with respect to cutting edge research and technologies being developed by such universities, including technology that has military applications.

(12) The universities of the United States provide fertile ground for nontraditional espionage given the open, international, and collaborative nature of most university research and the legitimate interest of universities in encouraging international collaboration.

(13) While the United States benefits from attracting the top research talent from around the world, universities nevertheless must take appropriate measures to ensure that China is not able to use academic collaboration to steal United States intellectual property or engage in other activities that might harm the national security of the United States.

(14) In response to the increased wave of nontraditional espionage over recent years, the Department of Justice launched a China Initiative in 2018. The goal of the China Initiative is to identify and prosecute individuals and entities engaged in economic and other nontraditional espionage, trade secret theft, hacking, and other crimes, while protecting critical infrastructure against external threats and combating covert efforts to influence the American public.

(15) Several recent criminal and civil enforcement actions taken by the Department of Justice highlight China's pervasive and illegal targeting of intellectual property and valuable research from United States universities, including the following:

(A) Dr. Qing Wang was a former employee of the Cleveland Clinic Foundation. He had received more than \$3,000,000 in grant funding from the National Institutes of Health (commonly known as "NIH"). Dr. Wang was charged in a criminal complaint with knowingly failing to disclose to NIH that he was Dean of the College of Life Sciences and Technology at the Huazhong University of Science and Technology (referred to in this subparagraph as "HUST") and received grant funds from the National Natural Science Foundation of China for some of the same scientific research funded by NIH. Dr. Wang also allegedly participated in the Thousand Talents Program, for which China provided \$3,000,000 in research support to enhance the facilities and operations at HUST. Federal law enforcement agencies arrested Dr. Wang in May 2020.

(B) Dr. James Patrick Lewis was a tenured professor at West Virginia University in the physics department from 2006 to 2019. In July 2017, Dr. Lewis entered into a contract of employment with the PRC through its Global Experts Thousand Talents Plan. In March 2020, Dr. Lewis pled guilty to 1 count of Federal program fraud.

(C) Anming Hu, an Associate Professor in the Department of Mechanical, Aerospace, and Biomedical Engineering at the University of Tennessee, Knoxville (commonly known as "UT"), allegedly engaged in a scheme to defraud the National Aeronautics and Space Administration (commonly known as "NASA") by concealing his affiliation with Beijing University of Technology (referred to in this subparagraph as "BJUT"). Hu's false representations to UT about his affiliation with BJUT caused UT to falsely certify to NASA that UT was in compliance with Federal law. In February 2020, Mr. Hu was indicted on Federal charges of wire fraud and false statements.

(D) Dr. Charles Lieber served as the Principal Investigator of the Lieber Research Group at Harvard University, which specialized in the area of nanoscience. Dr. Lieber had received more than \$15,000,000 in grant funding from NIH and the Department of Defense since 2008. Unbeknownst to Harvard University, beginning in 2011, Lieber allegedly became a "Strategic Scientist" at Wuhan University of Technology in China (referred to in this subparagraph as "WUT") and was a contractual participant in the Thousand Talents Plan from 2012 to 2017. Under the terms of the Thousand Talents contract, WUT paid Lieber \$50,000 per month, paid him living expenses of up to approximately \$158,000, and awarded him more than \$1,500,000 to establish a research lab at WUT. In return, Lieber was obligated to work for WUT for 9 months per year. Lieber lied about his involvement with WUT to both Harvard University and Federal investigators. In January 2020, Lieber was arrested and charged with making a materially false, fictitious and fraudulent statement.

(E) In January 2020, Yanqing Ye, a Chinese national, Lieutenant of the People's Liberation Army (referred to in this subparagraph as the "PLA"), and member of the CCP, was indicted on visa fraud, false statements, and acting as an agent of a foreign power without prior notification. Ye allegedly falsely identified as a student and lied about her ongoing military service at the National University of Defense Technology. While studying at Boston University's Department of Physics, Chemistry, and Biomedical Engineering, Ye continued to work as a PLA Lieutenant and completed assignments from PLA officers, including conducting research, assessing United States military websites, and sending United States documents and information to China.



(F) In January 2020, Zaoson Zheng, a Chinese national, was arrested at Logan Airport in Boston and charged with attempting to smuggle 21 vials of biological research to China. Zheng had allegedly entered the United States in 2018 on a J-1 visa and conducted cancer cell research at Beth Israel Deaconess Medical Center in Boston. Zheng admitted he stole the vials from a lab at Beth Israel, and that he intended to bring the vials to China, use them to conduct research in his own laboratory, and publish the results under his own name.

(G) In December 2019, the Van Andel Research Institute (referred to in this subparagraph as “VARI”) reached a settlement with the Department of Justice to pay \$5,500,000 to resolve allegations that it violated the law commonly known as the False Claims Act (section 3729 through 3733 of title 31, United States Code) by failing to disclose, in Federal grant applications and progress reports submitted to NIH, that the Chinese government funded 2 VARI researchers through grants. The VARI researchers were receiving research funding from Chinese sources while VARI was applying for and receiving NIH funding on their behalf.

(H) In September 2019, Yu Zhou and Li Chen were charged with crimes related to stealing exosome-related trade secrets. Zhou and Chen, spouses who worked in separate medical research labs at the Nationwide Children’s Hospital Research Institute, conspired to steal scientific trade secrets related to exosomes and exosome isolation from the Research Institute. The couple allegedly founded a company in China without the hospital’s knowledge. While employed at the Research Institute, they marketed products and services related to exosome isolation through their Chinese company. They also founded an American biotechnology company advertising products and services related to exosomes isolation, including a kit developed from a trade secret created at a Nationwide Children’s research lab. They eventually received more than \$876,000 and stock related to an asset purchase agreement involving the American company.

(I) In August 2019, Feng Tao, an associate professor at Kansas University, was indicted on Federal charges for concealing the fact that he was a full-time employee for Fuzhou University in China while doing research at Kansas University funded by the United States Government. Tao allegedly defrauded the United States Government by unlawfully receiving Federal grant money at the same time that he was employed and paid by a Chinese research university.

(J) Weiqiang Zhang, a Chinese national and United States legal permanent resident, acquired, without authorization, hundreds of rice seeds produced by his employer, Ventria Bioscience. Ventria is a Kansas biopharmaceutical research facility that develops genetically programmed rice to express recombinant human proteins, which are then extracted for use in the therapeutic and medical fields. Ventria spent millions of dollars and years of research developing its seeds and cost-effective methods to extract the proteins. Ventria used locked doors with magnetic card readers to restrict access to the temperature-controlled environment where the seeds were stored and processed. Zhang worked as a rice breeder for Ventria. In 2013, personnel from a crop research institute in China visited Zhang at his home in Kansas. Zhang drove the visitors to tour facilities in several States. United States Customs and Border Protection officers found seeds belonging to Ventria in the luggage of Zhang’s visitors as they prepared to leave the United States for China. In April 2018, Zhang was sentenced to 121 months in a Federal prison after having been convicted in

February 2017 of 1 count of conspiracy to steal trade secrets, 1 count of conspiracy to commit interstate transportation of stolen property, and 1 count of interstate transportation of stolen property.

(16) It remains a national security priority for the United States to protect the research and innovation developed in United States colleges and universities from misappropriation by any country, including the PRC.

#### SEC. 7502. DEFINITIONS.

In this title:

(1) AGENCY HEAD.—The term “agency head”, with respect to a covered research project, means the head of the covered agency providing the funding for the covered research project.

(2) COVERED AGENCY.—The term “covered agency” means—

(A) the Department of Defense;

(B) the Department of Energy; and

(C) an element of the intelligence community, as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(3) COVERED COUNTRY.—The term “covered country” means—

(A) the People’s Republic of China; and

(B) any other country designated by the Director, based on findings similar to the findings under subsection (a), which shall include consideration of—

(i) whether the country poses an existential threat to the economic interests and national security of the United States;

(ii) whether the country engages in persistent efforts to steal sensitive technology and proprietary information from companies, academic institutions, and other organizations of the United States through economic espionage and other forms of non-traditional espionage;

(iii) whether nontraditional forms of espionage serve as primary tools to further the goals of the country;

(iv) whether the nontraditional forms of espionage described in clause (iii) include—

(I) talent recruitment programs designed to recruit the country’s nationals to acquire knowledge about—and, often, steal—valuable and sensitive research at universities and research institutions abroad;

(II) luring foreign experts to the country to work on key strategic programs;

(III) using mergers and acquisitions or joint ventures as a means to gain access to high-level technology;

(IV) using cyber intrusions to steal information; and

(V) using front companies for state-affiliated entities to acquire export-controlled technology;

(v) whether the country has systematically sought to identify areas of United States innovation, education, and technology that could be replicated, stolen, or appropriated; and

(vi) whether the Office of the United States Trade Representative has placed the country on the Priority Watch List.

(4) COVERED PERSON.—The term “covered person” means an individual or institution of higher education that has a financial relationship with—

(A) a covered country;

(B) a political party within a covered country;

(C) a person who acts as an agent, representative, employee, or servant of a covered country; or

(D) a person who acts in any other capacity at the order or request, or under the direction or control, of a covered country.

(5) COVERED RESEARCH PROJECT.—The term “covered research project” means a research project at an institution of higher education—

(A) that is funded in whole or in part by a covered agency; and

(B) the subject of which is—

(i) an item subject to the Export Control Reform Act of 2018 (20 U.S.C. 4801 et seq.);

(ii) an item listed on the Commerce Control List (commonly known as the “CCL”) set forth in Supplement No. 1 to part 774 of title 15, Code of Federal Regulations; or

(iii) an item listed on the United States Munitions List under section 38(a)(1) of the Arms Export Control Act (22 U.S.C. 2778(a)(1)).

(6) DIRECTOR.—The term “Director” means the Director of National Intelligence.

(7) FINANCIAL RELATIONSHIP.—The term “financial relationship” means—

(A) any arrangement under which compensation is provided, directly or indirectly, by a covered country, or another entity or person described in subparagraph (B), (C), or (D) of paragraph (4), to—

(i) a covered person; or

(ii) an institution of higher education; or

(B) any direct or indirect ownership or investment interest by a covered country, or another entity or person described in subparagraph (B), (C), or (D) of paragraph (4), in an institution of higher education.

(8) INSTITUTION OF HIGHER EDUCATION.—The term “institution of higher education” has the meaning given the term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

#### SEC. 7503. APPROVAL OF COVERED PERSONS IN SENSITIVE GOVERNMENT-FUNDED RESEARCH PROJECTS.

(a) APPROVAL REQUIRED.—

(1) IN GENERAL.—A covered person may not participate in a covered research project unless the covered person applies for and receives approval from the agency head to participate.

(2) REQUIREMENTS.—An agency head may not approve a covered person to participate in a covered research project unless the agency head—

(A) performs a background check on the covered person in consultation with the Director; and

(B) collects any other relevant information about the covered person that the agency head determines appropriate, except any information pertaining to United States persons that the agency head is prohibited by law from collecting.

(b) PENALTY.—If an agency head determines that a covered person participating in a covered research project commenced on the date of enactment of this section has violated subsection (a), the agency head may—

(1) impose a probationary period, not to exceed 6 months, on the head of the project or the project;

(2) reduce, limit, or eliminate the funding for the project until the violation is remedied;

(3) permanently eliminate the funding for the project; or

(4) take any other action determined appropriate by the agency head.

#### SEC. 7504. DISCLOSURE OF RESEARCH ASSISTANCE FROM FOREIGN GOVERNMENTS.

(a) IN GENERAL.—Chapter 45 of title 18, United States Code, is amended by inserting after section 951 the following:

##### “§951A. Disclosure of research assistance from foreign governments

“(a) DEFINITIONS.—In this section—

“(1) the terms ‘agent of a foreign principal’ and ‘foreign principal’ have the meanings given those terms in section 1 of the Foreign Agents Registration Act of 1938, as amended (22 U.S.C. 611);

“(2) the term ‘covered research project’ has the meaning given the term in section 7502 of the Combating Chinese Purloining of Trade Secrets Act; and

“(3) the term ‘institution of higher education’ has the meaning given the term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).

“(b) FUNDING AND OTHER ASSISTANCE.—

“(1) FAILURE TO DISCLOSE FOREIGN FUNDING.—

“(A) OFFENSE.—It shall be unlawful for a person, while applying for or accepting a grant or other funding from an agency of the United States for a covered research project, to knowingly and willfully fail to disclose to the agency any grant or other funding that the person has received or will receive for the same project from a foreign principal or an agent of a foreign principal, including through an intermediary.

“(B) PENALTY.—Any person who violates subparagraph (A) shall be fined under this title, imprisoned for not more than 3 years, or both.

“(2) FAILURE TO DISCLOSE MATERIAL FACTS.—

“(A) OFFENSE.—It shall be unlawful for a person, while applying for or accepting a grant or other funding from an agency of the United States for a covered research project, to knowingly and willfully fail to disclose to the agency a material fact relating to a connection between a foreign country and the project that might substantially impact the decision of the agency to provide funding to the project, including the fact that a person providing any assistance, including financial assistance, to the project is—

“(i) a national of a foreign country;

“(ii) affiliated with an institution comparable to an institution of higher education of higher learning, or another organization, that is headquartered in or substantially funded by a foreign country; or

“(iii) engaging in research activities for the project in a foreign country.

“(B) PENALTY.—Any person who violates subparagraph (A) shall be fined under this title, imprisoned for not more than 1 year, or both.

“(3) INSTITUTIONS OF HIGHER EDUCATION.—Any institution of higher education that knowingly and willfully fails to disclose to the appropriate agency of the United States that an officer, agent, or employee of the institution of higher education violated this subsection shall be fined not more than \$1,000,000 for each such violation.

“(c) TRANSMISSION OF INFORMATION.—

“(1) OFFENSE.—It shall be unlawful for any person, while applying for or accepting a grant or other funding from an agency of the United States for a covered research project, to knowingly transmit or attempt to transmit information gained in violation of a contract to which the person is a party, including a contract regarding nondisclosure of information, employment, or the provision of goods or services, intending or knowing that the transmission will benefit a foreign principal or an agent of a foreign principal.

“(2) PENALTY.—Any person who violates paragraph (1) shall be fined under this title, imprisoned for not more than 10 years, or both.”

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 45 of title 18, United States Code, is amended by inserting after the item relating to section 950 the following:

“951A. Disclosure of research assistance from foreign governments.”

**SA 1947.** Ms. BALDWIN submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and Innovation in the National Science Foundation, to establish a regional

technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

Strike 2510 of division B and insert the following:

**SEC. 2510. COUNTRY OF ORIGIN LABELING ON-LINE ACT.**

(a) MANDATORY ORIGIN AND LOCATION DISCLOSURE FOR PRODUCTS OFFERED FOR SALE ON THE INTERNET.—

(1) IN GENERAL.—

(A) DISCLOSURE.—It shall be unlawful for a product that is required to be marked under section 304 of the Tariff Act of 1930 (19 U.S.C. 1304) or its implementing regulations to be introduced, sold, advertised, or offered for sale in commerce on an internet website unless the internet website description of the product—

(i)(I) indicates in a conspicuous place the country of origin of the product (or, in the case of multi-sourced products, countries of origin), in a manner consistent with the regulations prescribed under section 304 of the Tariff Act of 1930 (19 U.S.C. 1304) and the country of origin marking regulations administered by U.S. Customs and Border Protection; and

(II) includes, in the case of—

(aa) a new passenger motor vehicle (as defined in section 32304 of title 49, United States Code), the country of origin disclosure required by such section;

(bb) a textile fiber product (as defined in section 2 of the Textile Fiber Products Identification Act (15 U.S.C. 70b)), the country of origin disclosure required by such Act;

(cc) a wool product (as defined in section 2 of the Wool Products Labeling Act of 1939 (15 U.S.C. 68)), the country of origin disclosure required by such Act;

(dd) a fur product (as defined in section 2 of the Fur Products Labeling Act (15 U.S.C. 69)), the country of origin disclosure required by such Act; and

(ee) a covered commodity (as defined in section 281 of the Agricultural Marketing Act of 1946 (7 U.S.C. 1638)), the country of origin information required by section 282 of such Act (7 U.S.C. 1638a); and

(ii) indicates in a conspicuous place the country in which the seller of the product is located (and, if applicable, the country in which any parent corporation of such seller is located).

(B) ADDITIONAL REQUIREMENT.—The disclosure of a product's country of origin required pursuant to subparagraph (A)(i) shall not be made in such a manner as to represent to a consumer that the product is in whole, or part, of United States origin, unless such disclosure is consistent with section 5 of the Federal Trade Commission Act (15 U.S.C. 45(a)) and any regulations promulgated by the Commission pursuant to section 320933 of the Violent Crime Control and Law Enforcement Act of 1994 (15 U.S.C. 45a), provided that no other Federal statute or regulation applies.

(C) LIMITATION.—The provisions of this paragraph shall not apply to a pharmaceutical product subject to the jurisdiction of the Food and Drug Administration.

(2) CERTAIN DRUG PRODUCTS.—It shall be unlawful for a drug that is not subject to section 503(b)(1) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 353(b)(1)) and that is required to be marked under section 304 of the Tariff Act of 1930 (19 U.S.C. 1304) to be offered for sale in commerce to consumers on an internet website unless the internet

website description of the drug indicates in a conspicuous place the name and place of business of the manufacturer, packer, or distributor that is required to appear on the label of the drug in accordance with section 502(b) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 352(b)).

(3) OBLIGATION TO PROVIDE.—A manufacturer, distributor, seller, or private labeler seeking to have a product introduced, sold, advertised, or offered for sale in commerce shall provide the information identified in clauses (i) and (ii) of paragraph (1)(A) or paragraph (2), as applicable, to the relevant retailer or internet website marketplace.

(4) SAFE HARBOR.—A retailer or internet website marketplace satisfies the disclosure requirements under subparagraphs (i) and (ii) of paragraph (1)(A) or paragraph (2), as applicable, if the disclosure required under such clauses or paragraph (2), as applicable, includes the country of origin and seller information provided by a third-party manufacturer, distributor, seller, or private labeler of the product. If the retailer or internet website marketplace determines or has a reasonable basis to conclude that the information provided by a third-party manufacturer, distributor, seller, or private labeler to the retailer or internet website marketplace for a product is false or deceptive, the retailer or internet website marketplace shall not be required to disclose such false or deceptive information and shall be deemed to meet the disclosure requirements under such clauses (i) and (ii) or paragraph (2), as applicable, for that product.

(b) PROHIBITION ON FALSE AND MISLEADING REPRESENTATION OF UNITED STATES ORIGIN ON PRODUCTS.—

(1) UNLAWFUL ACTIVITY.—Notwithstanding any other provision of law, and except as provided for in paragraph (2), it shall be unlawful to make any false or deceptive representation that a product or its parts or processing are of United States origin in any labeling, advertising, or other promotional materials, or any other form of marketing, including marketing through digital or electronic means in the United States.

(2) DECEPTIVE REPRESENTATION.—For purposes of paragraph (1), a representation that a product is in whole, or in part, of United States origin is deceptive if, at the time the representation is made, such claim is not consistent with section 5 of the Federal Trade Commission Act (15 U.S.C. 45(a)) and any regulations promulgated by the Commission pursuant to section 320933 of the Violent Crime Control and Law Enforcement Act of 1994 (15 U.S.C. 45a), provided that no other Federal statute or regulation applies.

(3) LIMITATION OF LIABILITY.—A retailer or internet website marketplace is not in violation of this subsection if a third-party manufacturer, importer, distributor, or private labeler provided the retailer or internet website marketplace with a false or deceptive representation as to the country of origin of a product or its parts or processing.

(c) ENFORCEMENT BY COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of subsection (a) or (b) shall be treated as a violation of a rule prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) POWERS OF THE COMMISSION.—

(A) IN GENERAL.—The Commission shall enforce this section in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this section.

(B) PRIVILEGES AND IMMUNITIES.—Any person that violates subsection (a) or (b) shall